BEEKEEPER STUDIO DATA PROCESSING AGREEMENT

This Data Processing Agreement (“DPA”) forms part of the agreement for services (the “Principal Agreement”) between:

Customer (“Company” or “Controller”)

and

Beekeeper Studio, Inc. (“Processor”)

Company and Processor are referred to collectively as the “Parties”.

---

1. PURPOSE AND SCOPE

1.1 This DPA governs Processor’s processing of Personal Data on behalf of Company in connection with the Services.

1.2 The Parties intend this DPA to satisfy the requirements of Article 28 of the General Data Protection Regulation (“GDPR”) and other applicable Data Protection Laws.

1.3 Processor processes Personal Data solely as necessary to provide the Services described in the Principal Agreement and as further described in Schedule 1.

---

2. DEFINITIONS

2.1 “Data Protection Laws” means all applicable privacy and data protection laws including GDPR and applicable implementing laws.

2.2 “Personal Data”, “Processing”, “Controller”, “Processor”, “Data Subject”, and “Personal Data Breach” have meanings defined under GDPR.

2.3 “Subprocessor” means any third party engaged by Processor to process Personal Data on behalf of Company.

---

3. ROLES OF THE PARTIES

3.1 Company is the Controller of Company Personal Data.

3.2 Processor acts solely as a Processor.

3.3 For avoidance of doubt, where Beekeeper Studio software operates entirely on Company-controlled infrastructure and no Personal Data is transmitted to Processor systems, Processor shall not be considered to be processing Personal Data.

---

4. PROCESSING OF PERSONAL DATA

4.1 Processor shall:

(a) Process Personal Data only on documented instructions from Company;
(b) Process Personal Data only for purposes described in Schedule 1;
(c) Comply with all applicable Data Protection Laws.

4.2 Processor may process Personal Data as required by applicable law. Where permitted, Processor shall inform Company prior to such processing.

---

5. CONFIDENTIALITY AND PERSONNEL

5.1 Processor shall ensure that personnel authorized to process Personal Data:

(a) Are bound by confidentiality obligations;
(b) Receive appropriate training;
(c) Access Personal Data only as necessary to perform Services.

---

6. SECURITY MEASURES

6.1 Processor shall implement appropriate technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

6.2 Security measures are described in Schedule 2.

6.3 Processor shall regularly evaluate and update such measures.

---

7. SUBPROCESSORS

7.1 Company authorizes Processor to engage Subprocessors.

7.2 Processor shall:

(a) Maintain a current list of Subprocessors;
(b) Impose data protection obligations equivalent to this DPA;
(c) Remain liable for Subprocessor performance;
(d) Notify Company of material changes to Subprocessors.

7.3 Company may object to new Subprocessors on reasonable data protection grounds.

---

8. DATA SUBJECT RIGHTS

8.1 Processor shall assist Company in responding to Data Subject requests, including requests for access, rectification, erasure, restriction, or portability.

8.2 Processor shall promptly notify Company if it receives such request and shall not respond without Company authorization unless legally required.

---

9. PERSONAL DATA BREACH

9.1 Processor shall notify Company without undue delay and no later than seventy-two (72) hours after becoming aware of a Personal Data Breach affecting Company Personal Data.

9.2 Processor shall:

(a) Provide reasonable information about the breach;
(b) Cooperate with Company investigations;
(c) Assist with remediation and mitigation.

---

10. DATA PROTECTION IMPACT ASSESSMENTS

Processor shall provide reasonable assistance with Data Protection Impact Assessments and consultations with supervisory authorities where required.

---

11. AUDIT AND COMPLIANCE

11.1 Processor shall make available information reasonably necessary to demonstrate compliance.

11.2 Company may conduct audits subject to the following:

(a) Minimum 30 days written notice;
(b) No more than once annually unless required by law or breach investigation;
(c) Conducted during normal business hours;
(d) At Company's expense;
(e) Must not compromise security or confidentiality of other customers.

11.3 Processor may satisfy audit requests through independent third-party certifications or reports.

---

12. RETURN AND DELETION OF DATA

12.1 Upon termination of Services, Processor shall delete or return Personal Data within thirty (30) days, except where retention is required by law.

12.2 Backup copies shall be deleted according to normal backup rotation schedules.

---

13. INTERNATIONAL DATA TRANSFERS

13.1 Company acknowledges that Processor operates in the United States.

13.2 Where Personal Data is transferred outside the EEA or UK, transfers shall be governed by the European Commission Standard Contractual Clauses ("SCCs") and, where applicable, the UK International Data Transfer Addendum.

13.3 The SCCs are incorporated into this DPA by reference.

---

14. TELEMETRY AND OPERATIONAL DATA

14.1 Processor may process limited diagnostic, licensing validation, and operational metadata necessary to:

(a) Validate software licenses;
(b) Provide Workspace services;
(c) Maintain and secure the Services.

14.2 Any diagnostic or usage tracking from the desktop application is optional, anonymized, and opt-in.

---

15. LIABILITY AND LIMITATION

15.1 Each Party's liability under this DPA shall be subject to the limitations contained in the Principal Agreement unless prohibited by law.

---

16. CONFIDENTIALITY

Each Party shall keep confidential all non-public information obtained under this DPA.

---

17. TERM

This DPA remains in effect for the duration of the Principal Agreement and any period during which Processor processes Personal Data.

SCHEDULE 1 – PROCESSING DETAILS

Subject Matter:
Provision of Beekeeper Studio desktop software and Workspace services.

Nature and Purpose:
• License validation
• Workspace synchronization and storage
• Customer account and billing management
• Customer support services

Duration:
For the term of the Principal Agreement plus applicable retention periods.

Categories of Data Subjects:
• Customer employees and contractors
• Users of Workspace accounts
• Individuals referenced in customer support communications

Categories of Personal Data:
• Account registration details (name, email, billing details)
• Workspace data including database connection metadata
• Stored SQL queries and query history
• Customer support communications

Excluded Data:
Processor does not access or store database contents from customer databases.

SCHEDULE 2 – SECURITY MEASURES

Processor maintains security measures including:

Encryption
• TLS encryption for data in transit
• Encryption at rest for stored server data
• Application-level encryption for stored query text and connection credentials

Access Controls
• Role-based access controls
• Least privilege access policies
• Multi-factor authentication for administrative access

Infrastructure Security
• Secure cloud infrastructure
• Network segmentation
• Continuous vulnerability monitoring

Operational Security
• Security incident response program
• Logging and monitoring
• Regular security reviews

Data Handling
• Backup encryption
• Backup retention and rotation procedures

SIGNATURES

Customer:
Name:
Title:
Signature:
Date:

Beekeeper Studio, Inc.
Name: Matthew Rathbone
Title: CEO & President
Signature:
Date: 02 / 06 / 2026